REMARKS

In summary, claims 1-21 are pending, having previously canceled claims 33, 47-48 and previously withdrawn claims 22-32, 34-46 and 49-73 under a restriction requirement. Claims 1 and 21 are independent. Claims 1, 2, 8, 10, 12, and 21 are rejected under 35 U.S.C. § 102. Claims 3-7, 9, 11, and 13-20 are rejected under 35 U.S.C. § 103. A proposed amendment for Claim 1 is herein provided without adding new matter. Applicants respectfully traverse the rejections. Reconsideration in view of the foregoing amendment and following remarks is respectfully requested.

Telephone Conversation With Examiner

Applicant thanks Examiner Brown for the telephone conversation conducted on April 16, 2008. Proposed claim amendments were discussed. The cited art was discussed. No agreements were reached.

Examiner's Response to Previous Remarks

The Office Action comments that, "[i]t is unclear to the examiner how the computer program is able to perform the actions independent of 'any part of said cryptographic key' when it is employing 'key attributes' taken from said cryptographic key. . . . The examiner asserts that the applicant is merely separating the functions of the key into several actions taken by the code. . . . The examiner encourages the applicant to explain how taking key attributes and coding them into functions is different from breaking a key down into elements and coding them into functions." (Office Action, pp. 2-3).

In view of the instant Office Action and the aforementioned telephone conversation, it appears there is confusion between generating the computer program and applying the computer program. The cryptographic key may be accessed when generating the computer program. However, the cryptographic key is not exposed or accessed when applying the cryptographic key. When the computer program is applied to data without exposing or accessing the cryptographic key, the results are the same as if the cryptographic key were

applied to the data. For a more detailed explanation, Examiner is referred primarily to page 16, line 9 through page 18, line 13 of the Application.

Aucsmith concerns partitioning a program and secret and reassembling them by repetition. Aucsmith states that "[t]he secret . . . is 'partitioned' into subparts 101, and program 100 is unrolled into a number of subprograms 102 that operate with subparts 101." Aucsmith, col. 3, ll. 52-55. The Office Action cites an example provided by Aucsmith at column 3, lines 60-67. Therein, Aucsmith states that the program is A = X * 8. The secret (8) is partitioned into four parts of 2 and the program is partitioned (unrolled) to run four times to operate on the four parts of the secret, i.e., A = A + (X *2). The result of running the subprogram four times on the four parts of the secret (i.e. rolling-up the subprograms into the program), repeatedly adding A to itself , is A = X * 8, which is the original program and secret reassembled. Aucsmith is dealing with the parts and the whole of the program and secret just as it says it is. As a result, the secret and program are reassembled and exposed by running the last subprogram to roll-up the program.

In contrast, the claimed subject matter comprises a "computer program [] operable to perform said set of actions independent of a whole or any part of said cryptographic key." Application, Independent Claims 1 and 21. Properties about the key or part of the key or, may stored, or dynamically created code to represent the properties may be stored. Application, p. 16, ll.24-30 (the inventive program can store properties of the key or "[a]lternatively, instead of storing any information about the [key], the program could . . . represent it in memory by dynamically creating code that . . . produces [the property], where any portion of the program that needs to know the [property] simply executes the dynamically-created code instead of retrieving the [property] from memory. This is a simple example of how a program can be constructed to use a [key or part of a key] without storing the [key or part of a key] in memory or otherwise exposing the [key or part of a key] to discovery by a user.").

Determining the properties/attributes of a key, such as whether a particular number is odd or even, positive or negative, and determining the functions performed by an algorithm that applies the key to data in order to create a program independent of both the key and the

algorithm, is patentably distinct from keeping the key and algorithm, but partitioning them so the algorithm operates repetitively on parts of the secret to reassemble the secret and algorithm per Aucsmith.

The claimed invention clearly does not read on Aucsmith. In the claimed invention, the program has nothing to do with the key or any part of it. It doesn't have access to it and doesn't expose it in whole or in part. As recited in the specification, attributes of the key and the functionality of the algorithm using the key are observed and utilized so that no part of the key is exposed in memory. There is no simple partitioning and reassembling of the key and algorithm as in Aucsmith, which exposes the key and its parts in memory.

Even though Applicants believe the claimed invention as previously presented in patentable over the prior art, Applicants have proposed an additional amendment otherwise expressing the distinction.

Rejection of Claims 1, 2, 8, 10, 12, and 21 Under 35 U.S.C. § 102

Claims 1, 2, 8, 10, 12, and 21 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,892,899, issued to Aucsmith *et al.* (hereinafter referred to as "Aucsmith"). (Office Action, pp. 3-4.) Applicants respectfully traverse the rejection.

Aucsmith does not teach or suggest at least a "computer program . . . operable to perform said set of actions independent of the whole and any part of said cryptographic key." Claims 1 and 21. Likewise, Aucsmith does not teach or suggest the proposed amendments to independent claims 1 and 21:

> identifying a set of actions that are performed in the course of using a cryptographic algorithm to apply ~~a~~ the cryptographic key to first data;
>
> generating a first set of computer-executable instructions which includes instructions to perform said set of actions; and
>
> including said first set of computer-executable instructions in said computer program, wherein said computer program is operable to perform said set of actions independent of a whole and any part of said cryptographic key and without exposing or accessing any part of the cryptographic key.

Amended Independent Claims 1 and 21.

All of the foregoing remarks apply equally well to the present rejection of claims 1, 2, 8, 10, 12 and 21. As previously pointed out, Aucsmith clearly operates on (i.e. is dependent upon) the parts and the whole of a secret and algorithm, disassembling and reassembling them, thereby exposing the secret in whole and in part.

Claims 1, 4, 7, and 10 confirm Aucsmith's dependence on the key, in whole and in part. In Claim 1 Aucsmith states that "programming instruction blocks operat[e] on corresponding subparts of a secret distributed among them," while in Claim 4 Aucsmith states that a "method for executing a program that operates on a secret . . . compris[es] . . . executing a first unrolled subprogram of the program . . . operating on a first subpart of the secret; and executing a second unrolled subprogram of the program . . . operating on a second subpart of the secret." Aucsmith, Claim 4.

The presence of the dispersed key and reassembly of it by running the last subprogram remains problematic for security. In contrast, the claimed invention creates a program independent of the key, in whole and in part, that operates without exposing the key, in whole or in part, providing greater security than Aucsmith.

Thus, it is believed that independent claims 1 and 21 are allowable over Aucsmith. At least in view of their dependence on claim 1, it is similarly believed that claims 2-20 are also allowable over Aucsmith. Applicants respectfully request reconsideration of claims 1-21, as amended, and withdrawal of the rejection of claims 1, 2, 8, 10, 12 and 21 as being anticipated by Aucsmith.

Rejection of Claims 3-7, 9, 11, and 13-20 Under 35 U.S.C. § 103

Claims 3-7, 9, 11, and 13-20 are variously rejected under 35 U.S.C. § 103(a) as being unpatentable over Aucsmith in view of one or more of the following additional references: U.S. Patent No. 6,643,775, issued to Granger *et al.* ("Granger"); U.S. Patent No. 6,715,079 issued to Maytal ("Maytal"); U.S. Patent Application Publication No. 2002/0178412 in the name of Matsui ("Matsui"); U.S. Patent No. 5,912,972, issued to Barton ("Barton"); U.S. Patent No.

6,138,236, issued to Mirov ("Mirov") and U.S. Patent No. 5,758,293, issued to Frasier ("Frasier"). (Office Action, pp. 5-10.) Applicants traverse all rejections.

All foregoing remarks apply equally well to the rejections of dependent claims 3-7, 9, 11 and 13-20 under 35 U.S.C. 103. Accordingly, it is requested that the rejection of claims 3-7, 9, 11 and 13-20 under 35 U.S.C. 103 be reconsidered and withdrawn.

Amendments made herein as well as those previously made are without abandonment of subject matter. Applicant expressly reserves the right to, in the pending application or any application related thereto, reintroduce any subject matter removed from the scope of claims and introduce any subject matter not present in current or previous claims.

CONCLUSION

In view of the foregoing amendment and remarks, it is respectfully submitted that this application is in condition for allowance. Reconsideration of this application and an early Notice of Allowance are requested. In view of the pendency of this application for more than seven years, the Examiner is cordially invited to contact the undersigned representative of Applicants for any reason that Examiner believes may speed up allowance of the application

Date: June 17, 2008

/Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439